THAT WHICH IS CLAIMED IS:

1. A method of determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet; and

determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address.

2. The method of Claim 1, wherein the step of determining further comprises determining that the source IP address is spoofed if the source IP address is not bound to the source MAC address and the source MAC address is not associated with a gateway routing device.

3. The method of Claim 2, further comprising the steps of:

determining if the source MAC address is identified in an address resolution protocol (ARP) table as a MAC address of a routing device to determine if the source MAC address is associated with a gateway routing device.

4. The method of Claim 3, wherein the step of determining if the source MAC address is identified in an ARP table is preceded by the steps of:

determining if an IP address of a gateway routing device is to be added to a routing table;

sending an ARP request to the IP address of the gateway routing device;

receiving a response to the ARP request that identifies a MAC address of the gateway routing device;

updating the ARP table with the MAC address of the gateway routing device; and

identifying the MAC address in the ARP table as associated with a gateway routing device.

5. The method of Claim 2, further comprising the steps of:

determining IP addresses associated with the source MAC address in an address resolution protocol (ARP) table;

determining if the IP addresses associated with the source MAC address in the ARP table are associated with a gateway routing device to determine if the source MAC address is associated with a gateway routing device; and

determining that the source IP address is not spoofed if the source MAC address is associated with a gateway routing device.

6. The method of Claim 5, wherein the step of determining if the IP addresses associated with the source MAC address in the ARP table are associated with a gateway routing device comprises searching a routing table for the IP addresses to determine if any of the IP addresses are associated with a gateway routing device in the routing table to determine if the source MAC address is associated with a gateway routing device.

7. The method of Claim 1, wherein the step of evaluating further comprises the step of determining if an address resolution protocol (ARP) table entry indicates that the source MAC address is associated with the source IP address.

8. The method of Claim 7, wherein the step of determining if an ARP table entry indicates that the source MAC address is associated with the source IP address comprises the steps of:

identifying an entry in the ARP table corresponding to the source MAC address;

comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address; and

identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address.

9. The method of Claim 8, further comprising the steps of:

sending an ARP request to the source IP address if no entry in the ARP table is identified as corresponding to the source MAC address; and

incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request.

10. The method of Claim 9, further comprising the step of identifying the source IP address as not bound to the source MAC address if a response is not received to the ARP request.

11. The method of Claim 9, further comprising the step of discarding the packet if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

12. The method of Claim 9, further comprising the steps of:

determining if the source IP address is associated with a routing device;

forwarding the packet if the source IP address is associated with a routing device; and

discarding the packet if the source IP address is not associated with a routing device and if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

13. The method of Claim 7, further comprising the steps of:

determining if a packet having the source IP address has been previously received; and

forwarding the packet if a packet having the source IP address has not been previously received.

14. The method of Claim 13, further comprising the steps of:

sending an ARP request to the source IP address if a packet having the source IP address has not been previously received; and

incorporating an entry corresponding to the MAC address into the ARP table if a response is received to the ARP request.

15. The method of Claim 13, wherein the step of determining if an ARP table entry indicates that the source MAC address is associated with the source IP address comprises the steps of:

identifying an entry in the ARP table corresponding to the source MAC address;

comparing an IP address of the identified entry to the source IP address to determine if the IP address of the identified entry corresponds to the source IP address; and

identifying the source IP address as bound to the source MAC address at the source device if the IP address of the identified entry corresponds to the source IP address.

16. The method of Claim 15, further comprising the step of discarding the packet if no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

17. The method of Claim 13, further comprising the steps of:

determining if the source IP address is associated with a routing device;

forwarding the packet if the source IP address is associated with a routing device; and

discarding the packet if the source IP address is not associated with a routing device and no entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

18. The method of Claim 17, further comprising the step of forwarding the packet if an entry in the ARP table corresponding to the MAC address has an IP address which corresponds to the source IP address.

19. The method of Claim 1, further comprising the step of discarding the packet if it is determined that the packet has a spoofed source IP address.

20. The method of Claim 19, further comprising the step of discarding the packet if the MAC address is associated with more than a predefined number of IP addresses.

21. The method of Claim 20, wherein the predefined number of IP addresses is associated with the source device.

22. The method of Claim 20, wherein the predefined number of IP addresses is associated with a subnet associated with the MAC address.

23. The method of Claim 19, further comprising the step of discarding the packet if the source IP address is associated with at least one MAC address other than the source MAC address.

24. The method of Claim 19, further comprising the step of forwarding the packet if the source IP address indicates that the packet is a dynamic host configuration protocol (DHCP) request.

25. The method of Claim 24, wherein the step of forwarding the packet comprises forwarding the packet if the source IP address indicates that the packet is a dynamic host configuration protocol (DHCP) request and the contents of the packet indicate that the packet is a DHCP request.

26. The method of Claim 1, wherein a subnet of the source IP address matches a subnet from which the packet originated.

27. A method of doing business, comprising:

monitoring packets to determine if a source IP address of the packet is bound to a source MAC address of the packet at a source device of the packet so as to determine if the source IP address of the packet has been spoofed; and

identifying packets having a spoofed source IP address so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing spoofed source IP addresses.

28. The method of Claim 27, wherein the corrective action comprises the step of discarding the packet if the source IP address of the packet has been spoofed.

29. The method of Claim 28, wherein the corrective action further comprises logging MAC addresses of packets with spoofed source IP addresses.

30. The method of Claim 27, wherein the corrective action comprises notifying a system administrator of the subnet of the source device of the presence of a spoofed source IP address in a packet from the source device.

31. The method of Claim 27, wherein a destination device of the packet comprises a network attached storage device and wherein the corrective action comprises discarding the packet before the packet is forwarded to an Internet Protocol (IP) layer of the network attached storage devices so as to increase the availability of the network attached storage device in the event of a denial of service attack.

32. The method of Claim 27, further comprising the steps of:

monitoring packets from a source device to determine if the source device has more IP addresses bound to the MAC address of the source device than a predefined limit; and

identifying the source device as having more IP addresses bound to its MAC address than the predefined limit so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing spoofed source IP addresses bound to the MAC address of the source device.

33. The method of Claim 32, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing spoofed source IP addresses bound to the MAC address of the source device comprises discarding packets from the source device.

34. The method of Claim 33, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing spoofed source IP addresses bound to the MAC address of the source device comprises notifying a system administrator that the source device has more IP address bound to its MAC address than the predefined limit.

35. The method of Claim 32, further comprising the step of establishing the predefined limit based on characteristics of the source device.

36. The method of Claim 32, further comprising the step of establishing the predefined limit as a common limit for all devices on a subnet of the source device.

37. The method of Claim 27, further comprising the steps of:

determining if a source IP address is bound to a MAC addresses of more than one source device; and

identifying the source devices having the IP address bound to the MAC addresses so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing a spoofed source IP address bound to the MAC addresses of the source devices.

38. The method of Claim 37, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing a spoofed source IP address bound to the MAC addresses of the source devices comprises discarding packets from the source devices.

39. The method of Claim 37, wherein the corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing a spoofed source IP address bound to the MAC addresses of the source devices comprises notifying a system administrator that the IP address is bound to MAC addresses of more than one source device.

40. A system for determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

means for evaluating a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet; and

means for determining that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address.

41. The system of Claim 40, wherein the system comprises a routing device.

42. The system of Claim 40, wherein the system comprises a monitoring device.

43. The system of Claim 40, wherein the system comprises an endpoint device.

44. A system, comprising:

means for monitoring packets to determine if a source IP address of the packet is bound to a source MAC address of the packet at a source device of the packet so as to determine if the source IP address of the packet has been spoofed; and

means for identifying packets having a spoofed source IP address so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing spoofed source IP addresses.

45. A computer program product for determining if a packet has a spoofed source Internet Protocol (IP) address, comprising:

a computer readable media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code that evaluates a source media access control (MAC) address of the packet and the source IP address to determine if the source IP address of the packet has been bound to the source MAC address at a source device of the packet; and

computer readable program code that determines that the source IP address of the packet is spoofed if the source IP address is not bound to the source MAC address.

46. A computer program product, comprising:

a computer readable media having computer readable program code embodied therein, the computer readable program code comprising:

computer readable program code that monitors packets to determine if a source IP address of the packet is bound to a source MAC address of the packet at a source device of the packet so as to determine if the source IP address of the packet has been spoofed; and

computer readable program code that identifies packets having a spoofed source IP address so as to allow corrective action to be taken to reduce network degradation as a result of a denial of service attack utilizing spoofed source IP addresses.